Deploy the ASAv On the AWS Cloud

You can deploy the ASAv on the Amazon Web Sources (AWS) cloud.

About ASAv Deployment On the AWS Cloud

Note: The ASAv5 is NOT supported on AWS.

AWS is a public cloud environment that uses a private Xen Hypervisor. The ASAv runs as a guest in the AWS environment of the Xen Hypervisor. ASAv on AWS supports the following instance types:

- c3.large, c4.large, m4.large—2 vCPUs, 3.75 GB, 3 interfaces (1 management interface, 2 data interfaces)

  Note: Both the ASAv10 and ASAv30 are supported on the c3.large instance. However, we do not recommend deploying the ASAv30 on any large instances due to resource under-provisioning.

- c3.xlarge, c4.xlarge, m4.xlarge—4 vCPUs, 7.5 GB, 4 interfaces (1 management interface, 3 data interfaces)

  Note: Only the ASAv30 is supported on xlarge instances.

Note: The ASAv does not support the Xen Hypervisor outside of the AWS environment.

You create an account on AWS, set up the ASAv using the AWS Wizard, and chose an Amazon Machine Image (AMI). The AMI is a template that contains the software configuration needed to launch your instance.

Note: The AMI images are not available for download outside of the AWS environment.

Prerequisites for the ASAv and AWS

- Create an account on aws.amazon.com.
- License the ASAv. Until you license the ASAv, it will run in degraded mode, which allows only 100 connections and throughput of 100 Kbps. See Smart Software Licensing for the ASAv.
- Interface requirements:
  - Management interface
  - Inside and outside interfaces
  - (Optional) Additional subnet (DMZ)
- Communications paths:

  - Management interface—Used to connect the ASAv to the ASDM; can't be used for through traffic.
  - Inside interface (required)—Used to connect the ASAv to inside hosts.
  - Outside interface (required)—Used to connect the ASAv to the public network.
  - DMZ interface (optional)—Used to connect the ASAv to the DMZ network when using the c3.xlarge interface.
- For ASAv system requirements, see Cisco ASA Compatibility.

Guidelines and Limitations for the ASAv and AWS

Supported Features

- Deployment in the Virtual Private Cloud (VPC)
- Enhanced networking (SR-IOV) where available
- Deployment from Amazon Marketplace
- Maximum of four vCPUs per instance
- User deployment of L3 networks
- Routed mode (default)

Unsupported Features

- Console access (management is performed using SSH or ASDM over network interfaces)
- IPv6
- VLAN
- The ASAv5 with 100Mbps throughput
- Promiscuous mode (no sniffing or transparent mode firewall support)
- Multi-context mode
- Clustering
- ASAv native HA
- EtherChannel is only supported on direct physical interfaces
- VM import/export
- Amazon Cloudwatch
- Hypervisor agnostic packaging
- VMware ESXi

Configuration Migration and SSH Authentication

Upgrade impact when using SSH public key authentication—Due to updates to SSH authentication, additional configuration is required to enable SSH public key authentication; as a result, existing SSH configurations using public key authentication no longer work after upgrading. Public key authentication is the default for the ASAv on Amazon Web Services (AWS), so AWS users will see this issue. To avoid loss of SSH connectivity, you can update your configuration before you upgrade. Or you can use ASDM after you upgrade (if you enabled ASDM access) to fix the configuration.

Sample original configuration for a username "admin":

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
```

```
07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

To use the **ssh authentication** command, before you upgrade, enter the following commands:

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

We recommend setting a password for the username as opposed to keeping the **nopassword** keyword, if present. The **nopassword** keyword means that any password can be entered, not that *no* password can be entered. Prior to 9.6(2), the **aaa** command was not required for SSH public key authentication, so the **nopassword** keyword was not triggered. Now that the **aaa** command is required, it automatically also allows regular password authentication for a **username** if the **password** (or **nopassword**) keyword is present.

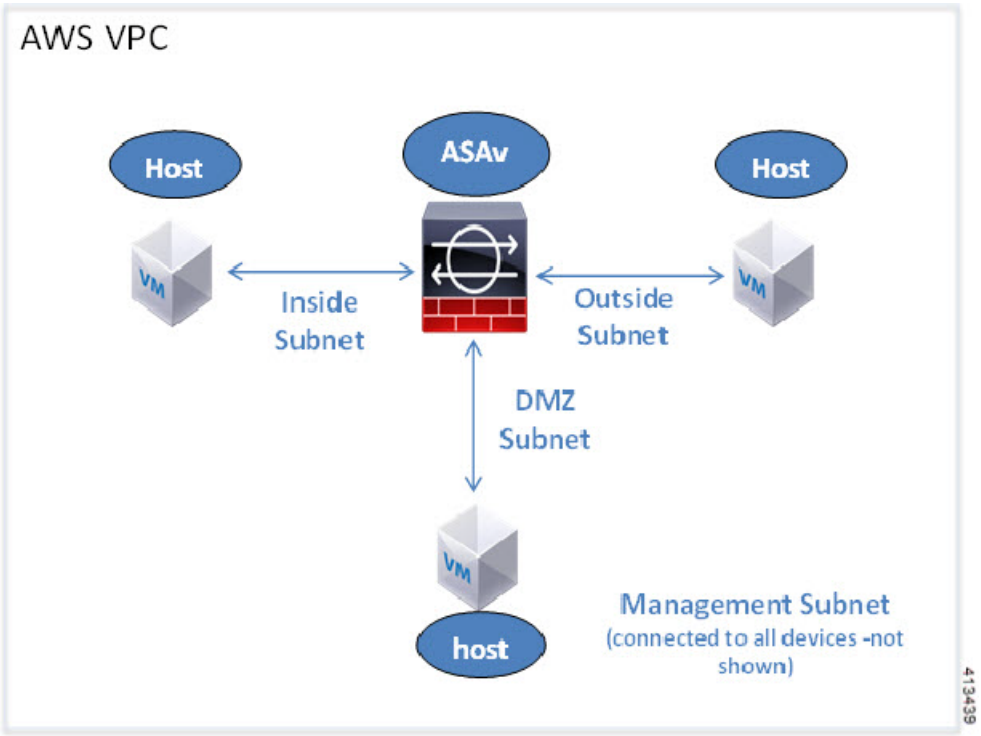
After you upgrade, the **username** command no longer requires the **password** or **nopassword** keyword; you can require that a user cannot enter a password. Therefore, to force public key authentication only, re-enter the **username** command:

```
username admin privilege 15
```

Sample Network Topology for ASAv on AWS

Figure 1 on page -47 shows the recommended topology for the ASAv in Routed Firewall Mode with four subnets configured in AWS for the ASAv (management, inside, outside, and DMZ).

Figure 1 Sample ASAv on AWS Deployment



Deploy the ASAv on AWS

The following procedure is a top-level list of steps to set up AWS on the ASAv. For detailed steps for setup, see Getting Started with AWS.

Procedure

1. Log into aws.amazon.com and choose your region.

   AWS is divided into multiple regions that are isolated from each other. The region is displayed in the upper right corner of your screen. Resources in one region do not appear in another region. Check periodically to make sure you are in the intended region.

2. Click **My Account > AWS Management Console**, and under Networking, click **VPC > Start VPC Wizard**, and create your VPC by choosing a single public subnet, and set up the following (you can use the default settings unless otherwise noted):

   - Inside and outside subnet—Enter a name for the VPC and the subnets.
   - Internet Gateway—Enables direct connectivity over the Internet (enter the name of the Internet gateway).
   - outside table—Add entry to enable outbound traffic to the Internet (add 0.0.0.0/0 to Internet Gateway).

3. Click **My Account > AWS Management Console > EC2**, and then click **Create an Instance**.

   - Select your AMI (for example Ubuntu Server 14.04 LTS).

     Use the AMI identified in the your image delivery notification.

   - Choose the instance type supported by the ASAv (for example, c3.large).
   - Configure the instance (CPUs and memory are fixed).
   - Under Advanced Details, add the Day 0 Configuration if desired. For the procedure for how to configure the Day 0 configuration with more information, such as Smart Licensing, see Prepare the Day 0 Configuration File, page 33.

     Sample Day 0 Configuration

```
! ASA 9.5.1.200
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 30
username admin nopassword privilege 15
username admin attributes
service-type admin
! required config end
! example dns configuration
dns domain-lookup management
DNS server-group DefaultDNS
! where this address is the .2 on your public subnet
name-server 172.19.0.2
! example ntp configuration
name 129.6.15.28 time-a.nist.gov
name 129.6.15.29 time-b.nist.gov
```

```
name 129.6.15.30 time-c.nist.gov
ntp server time-c.nist.gov
ntp server time-b.nist.gov
ntp server time-a.nist.gov
```

- Storage (accept the defaults).
- Tag Instance—You can create a lot of tags to classify your devices. Give it a name you can use to find it easily.
- Security Group—Create a security group and name it. The security group is a virtual firewall for an instance to control inbound and outbound traffic.

  By default the Security Group is open to all addresses. Change the rules to only allow SSH in from addresses you will be using to access your ASAv.
- Review your configuration and then click **Launch**.

4. Create a Key Pair.

   Give the key pair a name you will recognize and download the key to a safe place; the key can never be downloaded again. If you lose the key pair, you must destroy your instances and redeploy them again.
5. Click **Launch Instance** to deploy your ASAv.
6. Click **My Account > AWS Management Console > EC2 > Launch an Instance > My AMIs**.
7. Make sure that the Source/Destination Check is disabled per interface for the ASAv.

   AWS default settings only allow an instance to receive traffic for its IP address and only allow an instance to send traffic from its own IP address. To enable the ASAv to act as a routed hop, you must disable the Source/Destination Check on each of the ASAv's traffic interfaces (inside, outside, and DMZ).